

libcsdbg

1.15

Generated by Doxygen 1.8.5

Sun Jan 5 2014 16:11:36

Contents

1 Overview	1
1.1 Introduction	1
1.1.1 Description	1
1.1.2 Features	2
1.1.3 Licence and details	3
1.2 Obtaining the sources	3
1.3 Installation	4
1.3.1 Compile the sources (Unix/Linux)	4
1.3.2 Install a binary distribution (Unix/Linux)	6
1.3.3 Verify installation	7
1.4 Troubleshooting	8
1.4.1 Bug reports	8
1.4.2 How to contribute	8
1.5 Usage	9
1.5.1 5.1. Compiling with libcsdbg support	9
1.5.2 5.2. Configuring libcsdbg at runtime	9
1.5.3 5.3. Using the csdbg::tracer API	10
1.5.4 5.4. The Libcsdbg Debug Protocol (LDP)	13
1.5.5 5.5. Buffered output streams	14
1.5.6 5.6. Using the internal libcsdbg API	16
1.6 6. Examples and tutorials	17

1 Overview

1.1 Introduction

1.1.1 Description

Project **libcsdbg** is mainly a **C++ exception stack tracer**. When an exception is thrown, caught and handled, libcsdbg offers the tools to create and process the exception stack trace, the path the exception has propagated up the call stack, unwinding it, up to the section where it was handled. The traces are detailed with demangled function signatures and additional **addr2line** info (the source code file and line that each function was called). Libcsdbg will perform flawlessly with single and multithreaded (or multiprocess) programs, with any **dynamically linked shared object (DSO - Dynamic Shared Object)** and with any statically linked library. Additionally, libcsdbg helps the developer/tester create sophisticated stack traces **of any thread, at any given moment** during a process execution, or create **a dump of the call stacks of all threads** as a snapshot of the runtime call graph. This is very useful in cases of fatal errors, reception of terminating signals or process abortion/termination (such as segmentation faults).

In an object oriented programming paradigm, it's usually not enough to catch and handle an exception. It's essential to know at runtime, *where* in the code and under *what circumstances* the exception was thrown and also the path that the exception followed from the throw point up to the point where it was caught. Although much of this information can be embedded inside the exception object, this has several drawbacks, namely:

- It's not a complete solution

- It needs lots of code to keep track (the exception objects must have small footprint)
- It can't function with STL exceptions and integral types
- It's difficult to make it generic and portable

In Java, method **exception.printStackTrace** can provide this additional exception information, because the Java language is interpreted, not native, as C++ is. To implement this with GNU g++, libcsdbg exploits the g++ capability to generate and inject code for **function instrumentation**. Compiling code with the *-finstrument-functions* flag, commands g++ to inject code to call the instrumentation functions (csdbg::instrument_enter, csdbg::instrument_exit) at the beginning and end of all the instrumented functions. The compiled code is linked with libcsdbg that implements these two functions. At runtime, libcsdbg uses these functions to **transparently simulate** the call stack of each thread of execution within the debugged process, adding only **minimum overhead**. When an exception is thrown the actual thread stack is unwound until a catch section is found or until the process aborts, because of the unhandled exception. The stack simulator detects there is an exception being thrown and does not unwind, so the libcsdbg user can **print a stack trace**, at any place in the code (usually in the catch sections) or process the trace data any way seem fit.

Libcsdbg **transparently loads the symbol tables** of the executable and of any chosen dynamic shared objects, **demangles function symbols** to complete signatures and binds function names to **runtime addresses** (even for relocatable, position independent **DSO** symbols). Libcsdbg can use all the well-known objective code file formats (a.out, elf, coff, ecoff e.t.c), works with 32 and 64 bit systems and with both big and little endian architectures. The library API can easily be used as the base for your own instrumentation code.

The following is one of the traces produced when you execute example/csdbg_step1.cpp:

```
at thread 0x7f5e38289740 {
  at main
  at csdbg_extra::start(char const*, unsigned char) (csdbg_step1.cpp:151)
  at csdbg_extra::add_one_level(char const*, unsigned short) (csdbg_step1.cpp:90)
  at void csdbg_extra::middle<csdbg::string>(csdbg::string&, unsigned int&) (csdbg_step1.cpp:97)
  at csdbg_extra::bottom(char const*, unsigned long long volatile*, void (*) (double)) (csdbg_step1.cpp:107)
  at csdbg_extra::dso_main(char const*) (csdbg_step1.cpp:126)
  at csdbg_extra::dso_inner(char const*) (libcsdbg_test.cpp:55)
}
```

1.1.2 Features

This is a comprehensive, albeit not complete list of libcsdbg features:

- Create sophisticated exception stack traces (with addr2line support)
- Works with multithreaded processes and with multiprocess programs
- Create detailed **Posix thread** stack traces (with addr2line support)
- Full support for **Position Independent Code** (for DSO)
- Works with **generic throwables and user defined exception types**
- Support for most of the objective code formats (elf, a.out, coff, ecoff e.t.c)
- Support for both **32 and 64 bit** systems
- Support for both **big and little endian CPUs**
- Compiled/tested for x86, x86_64, ARM, AVR32, Leon

Project libcsdbg exports an extended, well documented and reusable **library API** to provide:

- Easy and minimal code interface, transparent library integration
- Easy library **runtime configuration**
- Transparent but configurable loading of symbol tables of any executable, DSO or other module

- Instrumentation algorithms add only **minimal overhead** and **memory footprint**
- The high level API provides **thread safety**
- Smart API to output trace or generic data to files or to network peers, with the use of **Libcsdbg Debug Protocol (LDP)**
- Library API can be used as the base for custom instrumentation code

Libcsdbg is currently available for **GNU/Linux/uClibc** platforms. There is development going on to provide a version for **Windows** (32 and 64 bit) systems (through **MinGW**) and Unix, **FreeBSD/OpenBSD/NetBSD** systems along with an **GNU autotools**-based build system and plugins for various **IDE** (Eclipse, Code::Blocks, e.t.c).

Project **jTracer** is a libcsdbg sister project, a portable **LDP** server implemented with Java. Each application that uses the libcsdbg LDP API can implement a jTracer client. This can be essential for **cross-platform** development with **embedded** devices and **development boards**. Most often target platforms such as these don't have a screen or other resources to visualize output and data collection during the development and debugging cycles is controlled at a workstation through ethernet or serial ports. Instead of cluttering the IDE, console or debugger with trace data, LDP is designed to isolate these generated data, collect them with jTracer (**even from multiple target hosts with diverse architectures**) and provide an easy way to navigate through them.

1.1.3 Licence and details

Libcsdbg is currently published as an Open Source project, licenced under the **GNU Library or Lesser General Public License version 3.0 (LGPLv3)**. **Tasos Parisinos** develops and maintains libcsdbg and the project documentation, while **Antonis Kalamaras** develops and maintains the build system. Version numbering uses three numbers, major, minor and subminor. **The current library version is 1.15**. Major library updates are related with multiple feature addition, significant changes in the library interface, major bug fixes or overall optimization. Minor library updates usually add minor features (or major features that were *almost* ready to be included in the major release, but didn't), minor bug fixes, typos and documentation updates or entities that need to be tested to gather feedback. Subminor releases are stable beta snapshots of the current code development status, with the last additions since the last minor update.

The following are locations essential to the development of libcsdbg:

- [Website](#)
- libcsdbg@sourceforge
- libcsdbg@freecode
- [Downloads](#)
- [Release News](#)
- [Forum](#)
- [Support](#)
- [jTracer website](#)
- jTracer@freecode

1.2 Obtaining the sources

The latest version of libcsdbg is 1.15 (release date January 5th 2014).

This version introduces the first implementation of the **instrumentation plugins** and the corresponding examples and tutorials. It also introduces the first edition of the project **user manual**. A plugin object is the way to declare a pair of instrumentation functions and register them with libcsdbg to be run upon function call and return. A plugin can be created by passing it the addresses of the instrumentation functions or by loading a plugin **module** (DSO) that implements and exports these two functions.

The names of the instrumentation functions (`__cyg_profile_func_enter` and `__cyg_profile_func_exit`) are hard-coded into g++, so only a unique implementation of these can exist at linkage time, therefore only one profiler can be used at a time. The plugin class is the fix to this shortcoming.

The latest **source** distribution is [libcsdbg-1.15.tar.bz2](#)

Alternatively, if you've already got the previous version (1.14) you can patch it to upgrade it to the latest release:

- [libcsdbg-1.14.tar.bz2](#)
- [upgrade-1.15.patch](#)

If you have both these files in the same directory, to apply the patch, execute:

```
tar -xjpf libcsdbg-1.14.tar.bz2
cd libcsdbg-1.14
patch -p1 < ../upgrade-1.15.patch
```

There are also **binary** distributions for 64 bit Linux (debug and release versions) compiled on **Ubuntu 13.04 TLS** (libbfd-2.22):

- [x86_64-linux-libcsdbg-1.15.tar.bz](#)
- [x86_64-linux-dbg-libcsdbg-1.15.tar.bz2](#)

The project **documentation** exists in the binary distributions and can be recreated (with [doxygen](#)) in the source code distributions. It can also be separately downloaded in **HTML** or as a single **hyperlinked PDF** document:

- [api-ref-libcsdbg-1.15.tar.bz2](#)
- [user-manual-libcsdbg-1.15.pdf](#)

Finally, if you want an overview of **all** project files check the libcsdbg [repository](#) at sourceforge.net. Click on any file's info icon and obtain its **SHA1** or **MD5** checksum to verify the file you've downloaded.

After you download any project file, remember to subscribe/follow libcsdbg in order to receive notification about new releases, updates, news, announcements and other libcsdbg related material in your mailbox. The easiest way to do so is to visit the [libcsdbg project page at freecode.com](#) and click on 'follow'

1.3 Installation

1.3.1 Compile the sources (Unix/Linux)

If you downloaded the source distribution, you need at least the following to build the library, the example executables and the project documentation:

- [GNU g++](#)
- [GNU make](#)
- [GNU binutils](#) (at least libbfd.so, strip and addr2line)
- UNIX standard tools such as rm, echo, touch, mkdir, cd, cp, ln, mv, grep, id, tar, ldconfig, wc, sudo
- You will need [doxygen](#) and [graphviz](#), to recreate the project documentation

Unpack the archive, unless you already have done that. If you want to recreate the documentation you must unpack the tarball in **/devel** (or change the paths in the doxygen configuration files (doc/docgen_html and doc/docgen_tex) with a simple text editor or **doxywizard**:

```
mkdir -p /devel
mv libcsdbg-1.15.tar.bz2 /devel
cd /devel
tar -xjpf libcsdbg-1.15.tar.bz2
```

Then compile and install it:

```
cd libcsdbg-1.15
sudo sh ./build
```

If you install as a simple user (not root) use of **sudo** is essential if you want to keep the default prefix (**/usr/local**). Installing in another prefix doesn't need root privilege, but the dynamic loader configuration file (**ld.so.conf**) will not be updated.

Currently **GNU autotools** are not supported but this is under development. The *build* script should compile without problems and install libcsdbg library, headers and other project files (examples e.t.c) with **/usr/local** as the prefix. For an overview of all *build* script options and modes of operation use:

```
sh ./build -h

Project libcsdbg installer
Usage: build [-c] [-u] [-m] [-s] [-d] [-h]

'build' will compile and install its target by default.
The following options change the default behaviour:

-c Clear the source tree (make clean)
-u Uninstall the package (make uninstall)
-m Compile but don't install
-s Don't parallelize compilation on multicore systems
-d Create/update the documentation (make doc)
-h Show this message
```

Although the *build* script can do all that you may need, to compile and install or uninstall, recreate the documentation or clear the source tree by calling the equivalent *Makefile* targets (in the **right** order), it is essential to describe these individual targets.

First of all clear the source tree from built binaries and documentation:

```
make clean
```

Compile the sources (the result binaries are stored in **./build**):

```
make
```

Install the library, header files and pkg-config file (under **/usr/local** by default):

```
make install
```

Then, if you want to compile and install the example executables and DSO, even in order to verify your installation (this is done by default by *build*), you must invoke:

```
make example-dso
make example
```

Optionally generate the documentation. This will create the **API reference** in **HTML** and the user manual in **LaTeX** and in **hyperlinked PDF** (all generated under **./doc**). To generate the PDF version of the manual you will need a running distribution of **LaTeX** and **pdflatex**, **makeindex** and **egrep**. To see the HTML documentation, just point a browser to *index.html* in the **./doc/api-ref-libcsdbg-\$VERSION** directory. The PDF manual *refman.pdf* will be located in the LaTeX directory of the distribution (**./doc/user-manual-libcsdbg-\$VERSION**). Just view and print it via the acrobat reader.

```
make doc
```

Finally, if you need to uninstall all libcsdbg-related files from your system:

```
make uninstall
```

As said earlier, no **autotools** support exists for the project but this is under way. So, currently all you can do is edit *Makefile* to change some options that may give you a headache. The *Makefile* options you may want to alter are:

\$PREFIX

Where to install libcsdbg

\$PLATFORM

The target prefix you need to cross compile the package (for example *mips-linux-*). It is used as the prefix for various binaries in the toolchain

\$LPATHS

Additional paths to search for DSO

\$IPATHS

Additional paths to search for header files

\$DOPTS

Define various preprocessor macros such as word size for the target machine achitecture (**the default is 64 bits**), the target machine endianness, debug or release mode, optimizations, include or discard modules e.t.c

\$GOPTS

Various g++ options such as target machine architecture, C++ standard used throughout compilation e.t.c

1.3.2 Install a binary distribution (Unix/Linux)

If you downloaded the binary distribution, you need the following to install and use libcsdbg:

- GNU **make**
- GNU **binutils** (at least libbfd.so (v2.22) and addr2line)
- UNIX standard tools such as rm, mkdir, cp, ln, ldconfig

Unpack the archive, unless you already have done that:

```
tar -xjpf x86_64-linux-dbg-libcsdbg-1.15.tar.bz2
```

```
- or -
```

```
tar -xjpf x86_64-linux-libcsdbg-1.15.tar.bz2
```

Then install it:

```
cd x86_64-linux-dbg-libcsdbg-1.15
sudo sh ./install
```

```
- or -
```

```
cd x86_64-linux-libcsdbg-1.15
sudo sh ./install
```

If you install as a simple user (not root) use of **sudo** is essential if you want to keep the default prefix (**/usr/local**). Installing in another prefix doesn't need root privilege, but the dynamic loader configuration file (**ld.so.conf**) will not be updated.

The *install* script should flawlessly install libcsdbg library, headers and other project files (examples e.t.c) using **/usr/local** as the prefix. If you want to alter the installation prefix, edit the *Makefile* and change **\$PREFIX** to a path of your choice. For an overview of other *install* script options and modes of operation use:

```
sh ./install -h

Project libcsdbg installer
Usage: install [-u] [-h]

'install' will install its target by default.
The following options change the default behaviour:

-u  Uninstall the package (make uninstall)
-h  Show this message
```

1.3.3 Verify installation

If all project components are correctly built and installed, the directory used as prefix (**/usr/local** by default) will have something like the following layout:

```
/usr/local/bin:
-rwxr-xr-x  1 root root    50851 Jan  5 15:36 csdbg_step1
-rwxr-xr-x  1 root root    56811 Jan  5 15:36 csdbg_step2
-rwxr-xr-x  1 root root    57151 Jan  5 15:36 csdbg_step3
-rwxr-xr-x  1 root root    67683 Jan  5 15:36 csdbg_step4
-rwxr-xr-x  1 root root    35929 Jan  5 15:36 csdbg_tut1
-rwxr-xr-x  1 root root    36191 Jan  5 15:36 csdbg_tut2
-rwxr-xr-x  1 root root    36311 Jan  5 15:36 csdbg_tut3
-rwxr-xr-x  1 root root    39343 Jan  5 15:36 csdbg_tut4
-rwxr-xr-x  1 root root    38057 Jan  5 15:36 csdbg_tut5

/usr/local/include:
drwxr-xr-x  2 root root   4096 Jan  5 15:36 csdbg
-rw-r--r--  1 root root    853 Jan  5 15:36 csdbg.hpp

/usr/local/include/csdbg:
-rw-r--r--  1 root root    700 Jan  5 15:36 call.hpp
-rw-r--r--  1 root root   7251 Jan  5 15:36 chain.hpp
-rw-r--r--  1 root root   5321 Jan  5 15:36 config.hpp
-rw-r--r--  1 root root   1591 Jan  5 15:36 exception.hpp
-rw-r--r--  1 root root   1291 Jan  5 15:36 filebuf.hpp
-rw-r--r--  1 root root   1900 Jan  5 15:36 name_space.hpp
-rw-r--r--  1 root root   3343 Jan  5 15:36 node.hpp
-rw-r--r--  1 root root    504 Jan  5 15:36 object.hpp
-rw-r--r--  1 root root   2277 Jan  5 15:36 plugin.hpp
-rw-r--r--  1 root root   5822 Jan  5 15:36 stack.hpp
-rw-r--r--  1 root root   2020 Jan  5 15:36 streambuf.hpp
-rw-r--r--  1 root root   2214 Jan  5 15:36 string.hpp
-rw-r--r--  1 root root    793 Jan  5 15:36 symbol.hpp
-rw-r--r--  1 root root   1908 Jan  5 15:36 symbol_table.hpp
-rw-r--r--  1 root root   2211 Jan  5 15:36 tcpsockbuf.hpp
-rw-r--r--  1 root root   1474 Jan  5 15:36 thread.hpp
-rw-r--r--  1 root root   3001 Jan  5 15:36 tracer.hpp
-rw-r--r--  1 root root   1020 Jan  5 15:36 util.hpp

/usr/local/lib:
drwxr-xr-x  3 root root    4096 Jan  5 15:36 modules
drwxr-xr-x  2 root root    4096 Jan  5 15:36 pkgconfig
lrwxrwxrwx  1 root root      31 Jan  5 15:36 libcsdbg.so -> /usr/local/lib/libcsdbg.so.1.15
-rwxr-xr-x  1 root root  163360 Jan  5 15:36 libcsdbg.so.1.15

/usr/local/lib/modules/libcsdbg:
-rwxr-xr-x  1 root root   32086 Jan  5 15:36 libcsdbg_test.so
-rwxr-xr-x  1 root root   13610 Jan  5 15:36 mod_null.so

/usr/local/lib/pkgconfig:
-rw-r--r--  1 root root    671 Jan  5 15:36 libcsdbg.pc
```

To validate that libcsdbg works correctly for your platform all you have to do is to execute the example executables *csdbg_step** or any of the tutorial executables *csdbg_tut**. The examples utilize most of the library API so they

provide best coverage, but the third and fourth examples are also **jTracer** clients and you will need a running server to verify the API. The installation directory (**\$PREFIX/bin**) of these executables must be in **\$PATH**. These programs will be dynamically linked with *libcsdbg.so* and with the example DSO *libcsdbg_test.so*, so their installation directories (**\$PREFIX/lib** and **\$PREFIX/lib/modules/libcsdbg**) must be in the **ld** path or in the **\$LD_LIBRARY_PATH** shell variable. You may need to invoke the following line, before you run any of the examples:

```
export LD_LIBRARY_PATH=/usr/local/lib:/usr/local/lib/modules/libcsdbg

- or in generic -

export LD_LIBRARY_PATH=$PREFIX/lib:$PREFIX/lib/modules/libcsdbg
```

The symbol table of the program is always loaded by *libcsdbg*. The user can select which DSO symbol tables to load and which to discard by declaring the **\$CSDBG_LIBS** shell variable as a ':' delimited list of POSIX extended regular expressions. The absolute path of each DSO is matched against each regexp. If **\$CSDBG_LIBS** is not set, all linked DSO symbol tables will be loaded. If it is set with a void value, all DSO are filtered out from instrumentation. You should only load the DSO that are compiled with *libcsdbg* support (see **Usage**). Loading non instrumented DSO is not a problem, except additional overhead. For example to run the example programs you must execute something like:

```
export CSDBG_LIBS=csdbg_test
```

1.4 Troubleshooting

1.4.1 Bug reports

Bugs are tracked in the **tickets** section of the *libcsdbg* site at **sourceforge.net**. Before submitting a new bug, first search through **all** the tickets (open and closed), if the same bug has already been submitted by others. If you are unsure whether or not something is a bug, you may ask help on the **users forums** first (subscription is **not** required, the forums are moderated).

So, you think you found a bug? You should report it either on the user forums or by sending an email to the project admin **tasos42@users.sourceforge.net**.

If you send only a (vague) description of a bug you are usually not very helpful and it will cost much more time to figure out what you mean. In the worst-case, your bug report may even be completely ignored, so always try to include the following information in your bug report:

- The version of *libcsdbg* you are using (use *pkg-config --modversion libcsdbg* if you are not sure)
- The name and version number of your operating system (*uname -a*)
- The *libcsdbg*-related shell and CLI variables
- All *libcsdbg* output (to the console, files, network) that is specific to the problematic scenario

The easiest way for us to fix bugs is if you can attach a small example that demonstrates the problem you have to the bug report, so we can reproduce it on our machines. Please make sure the example is valid source code and that the problem is really captured by the example. If you intend to send more than one file please zip or tar the files together into a single file for easier processing.

You can (and are encouraged to) add a patch for a bug. If you do so please use **PATCH** as a keyword in the bug entry form or in the email subject. If you have ideas how to fix existing bugs and limitations please discuss them on the **users forums**. For patches please use *diff -uprN* or include the files you modified.

1.4.2 How to contribute

Donate time

You can contribute your time by helping with programming, testing and filing bug reports, improving documentation, translations or by answering questions on the mailing list. We always welcome users whose only contribution is simply using libcsdbg, giving us feedback on how to improve it and telling others about it. Thank you for supporting libcsdbg.

Donate money

If you don't have time to help but do find libcsdbg useful, then please consider making a financial donation. This will help to pay the bills and motivate us to continue working on libcsdbg. You can do so using the Paypal account indicated on the project page at sourcefore.net, or contact us for other payment methods.

1.5 Usage

1.5.1 5.1. Compiling with libcsdbg support

Integration with libcsdbg is transparent and simple, just compile your code with some g++ mandatory flags and link with libcsdbg (-lcsdbg). From these g++ flags the most prominent are *-finstrument-functions* and *-g[format]*. You may need to invoke:

```
pkg-config --cflags libcsdbg

-fPIC
-g
-finstrument-functions
-finstrument-functions-exclude-file-list=/usr/include
-finstrument-functions-exclude-file-list=iostream
-finstrument-functions-exclude-file-list=ios
-finstrument-functions-exclude-file-list=istream
-finstrument-functions-exclude-file-list=ostream
-finstrument-functions-exclude-file-list=/usr/local/include/csdbg
-I/usr/local/include
```

to see **all** the additional flags you must pass to the compiler. Similarly:

```
pkg-config --libs libcsdbg

-L/usr/local/lib
-L/usr/local/lib/modules/libcsdbg
-lcsdbg
-ldl
-lbfd
-lpthread
```

will print the flags you must pass to the linker. You may need to add **\$PREFIX/lib/pkgconfig** to your pkg-config path.

Stack traces created with libcsdbg can only contain calls to functions that are instrumented by libcsdbg. For example if you write code for an application and instrument that code with libcsdbg only these functions you instrument will appear in traces. If you link your application with third-party DSO, the DSO function calls will not appear in the trace by default! You need to recompile those DSO to add libcsdbg support. As a rule of thumb, you should recompile code to add support for libcsdbg **if that code throws exceptions** and if it is essential to you to see how those exceptions propagated inside the module call graph.

Even if you don't call a single API method, if libcsdbg is compiled with debug support, it is easy to see if everything linked properly by just running your application: libcsdbg will at least attempt to load its symbol table and it will print various debug messages

1.5.2 5.2. Configuring libcsdbg at runtime

Before you run a program linked with libcsdbg there are some things you may want to configure, apart from the dynamic linker path, to help libcsdbg decide what to load and what to ignore, as well as some other runtime configuration tokens.

The symbol table of the program is always loaded by libcsdbg. The user can select which DSO symbol tables to load and which to discard by declaring the `$CSDBG_LIBS` shell variable as a ':' delimited list of POSIX extended regular expressions. The absolute path of each DSO is matched against each regexp. If one matches then the symbol table of the DSO is loaded to the libcsdbg namespace and the DSO functions are instrumented throughout execution. If `$CSDBG_LIBS` is not set, all linked DSO symbol tables will be loaded. If it is set with a void value, all DSO are filtered out from instrumentation. You should only load DSO that are compiled with libcsdbg support. Loading non instrumented DSO is not a problem, apart from additional overhead. For example to run the example programs you must execute:

```
export CSDBG_LIBS=csdbg_test
```

Another shell variable you may care to set is `$CSDBG_PEER`. In case you utilize any `csdbg::tcpsockbuf` object to implement an `LDP/jTracer client` this variable tells these objects the default server **IP address** and **TCP port**, if not set programmatically (as the constructor arguments). It must be formatted as `IPAddress[:TCPport]`. If the port is omitted the default LDP port (**4242**) is assumed. Generally, to get the value of such shell variables, parsed to their components, you need to use the `csdbg::tracer::getenv` method instead of the equivalent `libc` function.

Libcsdbg can also accept command line arguments. To avoid conflicts with the application and its command line arguments, the ones for libcsdbg are prefixed with `-csdbg-`. To feed those arguments to libcsdbg you must call, early in your code the `csdbg::tracer::init` method. This method parses the command line argument vector, identifies the arguments for libcsdbg, canonicalizes (removes the `-csdbg-` prefix), stores them internally and removes them from the vector, so the application never knows they were there. These arguments may just be flags or pass values to the library. Currently no such argument is utilized and the mechanism is there only for the users to use, but in the future the runtime configuration of libcsdbg will be affected by them and/or a configuration file.

1.5.3 5.3. Using the `csdbg::tracer` API

To be able to do anything with libcsdbg, even when you use its higher level objects (`csdbg::filebuf`, `csdbg::tcpsockbuf` e.t.c) you first need to obtain a `csdbg::tracer` object. The word is obtain, not create, because the class constructors, destructor and assignment operator are not public. The class itself provides you with interfacing tracer objects. You must call the `csdbg::tracer::interface` static method, as seen in the following snippet, to obtain a pointer to an interfacing tracer object.

```
using namespace csdbg;

tracer *iface = tracer::interface();
if ( unlikely(iface == NULL) )
    ; // abort
```

If this call returns `NULL`, that means that library initialization failed to load at least one symbol table. You should check the debug and generic output to see why this occurred. For example this can happen if all modules and the executable itself are stripped of symbols! You don't need to release or otherwise clear the obtained interface object after you are done. The library will take care of it internally.

Read the code and comments of the **Examples**, this will help you understand how to use libcsdbg, how to interface with it with code and use its facilities. The interface is really very simple and usually it takes **one or two lines of code to produce a trace!**

1.5.3.1 5.3.1 Exception stack traces

The best place to create and output (or process) an exception stack trace is in the **catch** section that is handling it. There are two ways to output such a trace. The first is to feed the tracer object to an STL output stream, using the insertion operator, for example:

```
using namespace csdbg;

tracer *iface = tracer::interface();
if ( unlikely(iface == NULL) )
    return;

try {
    ...
```

```

}

catch (exception &x) {
    std::cout << x << "\r\n" << *iface << "\r\n";
}

iface->unwind();

```

This is the simplest way possible! Although inside the tracer object lots of things are happening behind the scenes, things that can throw exceptions, you don't need to worry, they are taken care of internally. Moreover the output to an STL stream is **atomic** in the scope of the library (no other library output method will interleave). The other way to get the stack trace of the currently handled exception is to call the interface tracer object to store it in a `csdbg::string` buffer, as in the following example:

```

using namespace csdbg;

tracer *iface = tracer::interface();
if ( unlikely(iface == NULL) )
    return;

try {
    ...
}

catch (exception &x) {
    try {
        string buf;
        iface->trace(buf);
    }

    catch (...) {
    }
}

iface->unwind();

```

As you see in this last example, creating a stack trace in this way may throw exceptions that are the caller's responsibility to handle. The call to `csdbg::tracer::unwind` is only **mandatory** when the exception stack trace is ignored (in order to dispose that stored trace). If you don't properly unwind the simulated stack, the stored trace will mess with the next attempt to obtain a stack trace. Nevertheless, if the trace was actually created, a call to `unwind` doesn't affect the tracer object state at all (nothing to dispose), so it is not an error to call it once or even more times even when the trace was produced. Mind you, all calls to `csdbg::tracer::trace` even from the `std::ostream` insertion operator **unwind** the stack on their own.

A final point is, if you code a function to do the trace creation and output, this function must not be instrumented, otherwise it will corrupt the exception stack trace. Here's an example:

```

using namespace csdbg;

void foo(exception&) __attribute__((no_instrument_function));

void foo(exception &x)
{
    tracer *iface = tracer::interface();
    if ( unlikely(iface == NULL) )
        return;

    try {
        string buf;
        iface->trace(buf);
    }

    catch (...) {
    }
}

try {
    ...
}

catch (exception &x) {
    foo(x);
}

iface->unwind();

```

Due to C++ polymorfism **all subclasses of `csdbg::string`** (including the buffered output stream types of the library, like `csdbg::filebuf`, `csdbg::tcpsockbuf` and those to come) work in the same way!

1.5.3.2 5.3.2 Thread stack traces

You can create a thread stack trace anywhere in your code, at any moment of execution. You can create a stack trace for the currently running thread or for any process thread, running, stopped, resumed or blocked with a call at the two argument variant of `csdbg::tracer::trace` as in the next example:

```
using namespace csdbg;

tracer *iface = tracer::interface();
if ( unlikely(iface == NULL) )
    return;

string buf;
iface->trace(buf, pthread_self());
```

In case you have stored the thread ID of any thread, you then can obtain its stack trace from any other thread. Although the `libcsdbg` higher lever (interface) library calls are thread safe, you should be vigilant for data races that *you* may create. Another consideration, is that the above code **can** throw some exceptions, that of course you need to handle somewhere. `Libcsdbg` maintains a list of all simulated threads. There are three tracer methods to obtain the `csdbg::thread` object descriptor for a thread:

- `csdbg::tracer::current_thread` - Get the current thread descriptor
- `csdbg::tracer::thread_by_id` - Get the thread descriptor for a specific ID
- `csdbg::tracer::thread_at` - Get the thread descriptor at an offset in the thread enumerator

This is an example of creating a stack trace for the third thread in the list:

```
using namespace csdbg;

tracer *iface = tracer::interface();
if ( unlikely(iface == NULL) )
    return;

thread *thr = iface->thread_at(2);
string buf;
iface->trace(buf, thr->handle());
```

Another version of thread stack tracing is to create a batch trace for all the threads within a process. This feature is delivered by calling the method `csdbg::tracer::dump`. This can prove **extremely** helpful when you want to debug an application that has totally crashed. Instead of loading and debugging the **core dump** (if the OS supports this!) you can solve the problem quicker by taking a look at the thread stack traces, to see what each was doing (and what the then executing thread was doing) before the program crashed. Here's an example scenario:

1. The application setups and registers a handler for the **SIGSEGV** signal
2. A thread execution creates a **memory access violation**
3. The process receives a **SIGSEGV** because of the segmentation fault
4. The registered handler creates a stack trace dump for all the threads and stores it in a file using a `csdbg::filebuf` object
5. The process aborts

There are additional methods in the `csdbg::tracer` public API, they are designed to be called by the instrumentation functions (these functions are not part of the **csdbg** namespace, so they too need to obtain a tracer interface and use its public methods). These methods are used for thread management and symbol lookup and they **may** be called by the library user. One of them, `csdbg::tracer::cleanup_thread`, is specifically for the library user. This method should be called from **thread cancellation handlers** to release resources. If you don't cleanup the thread descriptor, though it becomes useless when the actual thread has exited, it continues to occupy memory and will also inject junk, empty traces in dumps or in explicit trace requests. This method may also be called just before a thread exits. If you don't call `cleanup_thread`, it is not a bug, it's just poor coding. When you have called this method you should call no more methods for the deleted thread ID. Again, this will be handled by the library, but again, it is poor coding.

1.5.4 5.4. The Libcsdbg Debug Protocol (LDP)

Ok, you have created some traces and learned how to output them to a console or store them in buffers. **LDP (Libcsdbg Debug Protocol)** is an application level protocol designed to transmit trace data, together with other, process, thread and exception descriptive data, through any media and transport layer protocol (**TCP/IP**, **UDP/IP** e.t.c). LDP is a **unidirectional, client-server** protocol. Unidirectional because only the client sends (trace) data to the server, the server need not acknowledge or reply in any way. The only role that the server plays in LDP, is to collect these data from multiple (and possibly of variant architecture and OS) client peers and store them or let a user collectively navigate through them and process them. LDP is designed as a message oriented protocol (like **HTTP**). A single connection, kept alive, can be used to send multiple messages but this is not mandatory, it is up to the implementation. Nevertheless, two LDP messages are not connected in any way and can be thought as two separate LDP sessions. This is a pseudo-BNF description of a message:

- The message consists of a **head** and a **body** separated by an empty line (`\r\n`)
- The **head** consists of a number of **headers**
- Each **header** is formatted as `'key: value\r\n'`
- Header numeric values are **hexadecimal** (no 0x prefix)
- The message **body** is the whole trace
- The message is terminated by an empty line

This is the generic layout:

```
key1: value1\r\n
key2: value2\r\n
...
keyN: valueN\r\n
\r\n
trace data\r\n
\r\n
```

The mandatory protocol headers are for:

- executable absolute path
- process ID
- thread ID
- timestamp (in microseconds)

The non mandatory protocol headers are for:

- exception data
- other, user and OEM headers

The following is an LDP message created by example/csdbg_step4.cpp:

```
path: /usr/local/bin/csdbg_step4
pid: 7064
tid: 7f85dc174700
tstamp: 4ee23066d8960

at thread 0x7f85dc174700 {
  at csdbg_extra::pthread_main(void*)
  at csdbg_extra::start(char const*, unsigned char) (csdbg_step4.cpp:139)
  at csdbg_extra::add_one_level(char const*, unsigned short) (csdbg_step4.cpp:158)
  at void csdbg_extra::middle<csdbg::string>(csdbg::string&, unsigned int&) (csdbg_step4.cpp:165)
  at csdbg_extra::bottom(char const*, unsigned long long volatile*, void (*)(double)) (csdbg_step4.cpp:176)
}
```

Project **jTracer** is a libcsdbg sister project, a portable LDP server implemented with Java. Each application that uses the libcsdbg LDP API can implement a jTracer client. This can be essential for **cross-platform** development with **embedded** devices and **development boards**. Most often target platforms such as these don't have a screen or other resources to visualize output and data collection during the development and debugging cycles is controlled at a workstation through ethernet or serial ports. Instead of cluttering the IDE, console or debugger with trace data, LDP is designed to isolate these generated data, collect them with jTracer (**even from multiple target hosts with diverse architectures**) and provide an easy way to navigate through them.

1.5.5 5.5. Buffered output streams

Subclassing the abstract class `csdbg::streambuf` is the standard way to create objects that output traces and other data to various media. A `streambuf`-derived object is both a string buffer (an object of class `csdbg::string`) and an output stream. The media that are supported are those that can be handled with an integer descriptor (files, character devices, terminals, sockets, pipes e.t.c). The libcsdbg project is currently shipped with two `streambuf` subclasses, `csdbg::filebuf` is used to output traces to files and `csdbg::tcpsockbuf` is used to transmit traces through a TCP/IP network. Other classes to support serial terminals, UDP/IP and Unix sockets, pipes, FIFOs and other will be added in the future. Class `streambuf` apart from providing the common base functionality it also implements a part of the **LDP (Libcsdbg Debug Protocol)**. These classes are not thread safe, the caller must implement thread synchronization.

1.5.5.1 5.5.1 Using `csdbg::filebuf`

A `csdbg::filebuf` object is a buffered output stream used to output **LDP (Libcsdbg Debug Protocol)** data (protocol headers and traces) or generic data to a file. This class is not thread safe, the caller must implement thread synchronization. A `filebuf` object inherits all the `csdbg::string` methods designed for text manipulation (append, clear, set e.t.c). You use these methods to process the buffer data, or the `csdbg::tracer` methods to store traces to the buffer. Then, you may open the underlying file stream and flush/clear the buffer. You can re-fill and re-flush as many times as you wish before you close the `filebuf`. Closing is just the opposite of open, it doesn't release the object and its buffer, so you may re-open it. The steps to use a `filebuf` object are:

1. Create a `filebuf` object for a path
2. Open the file
3. Append/set text data in the buffer
4. Flush the buffer
5. Repeat steps 3-4 until completion
6. Close
7. Repeat steps 2-6 until completion
8. Release the object

Step 2 in this list can be inserted anywhere within steps 2-4, you don't need to open the file in order to process its buffer, it must be opened before you flush the buffer. To name files in an unambiguous way, method `csdbg::filebuf::unique_id` can come in handy. It takes a printf-style format string (the default format is `%e_%p_%t_%s`) and uses the following specifiers:

- `%e` - executable name
- `%a` - executable absolute path
- `%p` - process ID
- `%t` - thread ID
- `%s` - timestamp (in microseconds)

The following is an example of using the filebuf class:

```
using namespace csdbg;

tracer *iface = tracer::interface();
if ( unlikely(iface == NULL) )
    return;

/* Log a trace to a file, with a unique, trace describing name */
string *nm = filebuf::unique_id("%e_%s");
nm->append(".trace");
filebuf fout(nm->cstr());

/* Add a header that describes the trace */
fout.header();
fout.append("\r\n");
iface->trace(fout, pthread_self());
fout.append("\r\n");

fout.open();
fout.flush();
fout.close();
```

1.5.5.2 5.5.2 Using csdbg::tcpsockbuf

A csdbg::tcpsockbuf object is a buffered output stream than can be used to implement the client side of the **LDP (Libcsdbg Debug Protocol)** or a generic **TCP/IP client socket**. Nevertheless, this class is optimized for LDP and generally for **unidirectional** protocols. If you need to implement a **bidirectional** protocol you must subclass tcpsockbuf. This class is not thread safe, the caller must implement thread synchronization. A tcpsockbuf object inherits all the csdbg::string methods designed for text manipulation (append, clear, set e.t.c). You use these methods to process the buffer data, or the csdbg::tracer methods to store traces to the buffer. Then, you may connect the socket to its peer and flush/clear the buffer. You can re-fill and re-flush as many times as you wish before you close/disconnect the tcpsockbuf. Disconnecting (closing) or shutting down the socket is just the opposite of open/connect, it doesn't release the object and its buffer, so you may re-connect it. The steps to use a tcpsockbuf object are:

1. Create a tcpsockbuf object for a peer IP address and TCP port
2. Connect to the peer
3. Append/set text data in the buffer
4. Flush the buffer
5. Repeat steps 3-4 until completion
6. Disconnect
7. Repeat steps 2-6 until completion
8. Release the object

Step 2 in this list can be inserted anywhere within steps 2-4, you don't need to connect the socket in order to process its buffer, it must be connected before you flush the buffer. The following is an example of using the tcpsockbuf class:

```
using namespace csdbg;

tracer *iface = tracer::interface();
if ( unlikely(iface == NULL) )
    return;

tcpsockbuf *client = NULL;
chain<string> *peer = tracer::getenv(csdbg::g_peer_env);
if (peer == NULL)
    client = new tcpsockbuf();
else
    client = new tcpsockbuf(peer->at(0)->cstr());

/* Log a trace to a socket connected to an LDP server at port 4242 */
client->header();
client->append("\r\n");
iface->trace(*client, pthread_self());
```

```

client->append("\r\n");

client->open();
client->flush();
client->close();

```

1.5.6 5.6. Using the internal libcsdbg API

Although now you know everything you need, to produce and process any kind of **stack trace**, some libcsdbg types may still come in handy, for other, more generic purposes, although these types are quite specific and optimized for the project. This is why, some of these classes have some rather tricky details, so instead of getting lost in the code and comments to get an idea, some of them are shortly described here, with some of their most uncommon features.

Class csdbg::exception

This type is used internally by libcsdbg to propagate and process errors. It is also used by the library to report internal errors to the user. Users may use it or even subclass it for their own needs. An exception object can be constructed using **printf-style formatting** and a variable argument list (for its error message). Inside the constructor, copy constructor and assignment operator other formatting or allocation exceptions may be recursively thrown but they are internally caught and silently ignored. In these cases the object is still safe to use by ignoring its error message. The std::ostream insertion operator implementation and all exception methods take this into account. Although an exception object is not thread safe by itself, all overloaded std::ostream insertion operator implementations that output exceptions synchronize thread access.

Class csdbg::string

A string object is mainly used to create trace text. Text is easily appended using **printf-style format** strings expanded with variable argument lists. Memory is allocated in blocks (aligning) to reduce overhead when appending multiple small strings. It is comparable against **POSIX extended regular expressions**. By creating traces in string buffers it is easy to direct library output to any kind of stream (console, file, serial, network, plugin, device e.t.c). Apart from traces a string can be used for generic dynamic text manipulation. This class is not thread safe, the caller must implement thread synchronization.

Data structure classes csdbg::node, csdbg::chain and csdbg::stack

A node can be instantiated only through the public methods of a chain or stack object. When a node is released it also calls delete (not delete[]) on its data pointer, unless it's previously **detached**. Therefore each node must point to a single T and not a T[] (allocated with operator new, not new[]). If a node is constructed with a pointer to a T[], memory leaks are bound to happen. When a node is copied or assigned, only its data are copied (not the position in its container). The data copy works for any type (integral or user defined) except arrays. Data copying invokes T(const T&) or T::operator=(const T&), exceptions thrown from these methods are not handled by the node nor its container, they are just propagated up the call stack.

The chain supports shared data (multiple chains can point to the same data) but it is not thread safe, callers should synchronize thread access. This implementation doesn't allow a node with a NULL or a duplicate data pointer. A node can be **detached** (dispose the node without deleting its data) or **removed** (dispose both node and data). A chain can be traversed using simple callbacks and method csdbg::chain::foreach.

The stack supports shared data (multiple stacks can point to the same data) but it is not thread safe, callers should synchronize thread access. This implementation doesn't allow a node with a NULL or a duplicate data pointer. A stack can be traversed using simple callbacks and method stack::foreach. Apart from the legacy **push/pop** functions, node data can be accessed using stack offsets.

Class csdbg::symbol_table

A symbol_table object can load code from executables or dynamic shared objects with absolute addressing or position independent. It supports all the binary formats supported by the **libbfd backends** on the host (or target) machine (elf, coff, ecoff e.t.c). To optimize lookups the symbol table (as structured in libbfd) is parsed, the non-function symbols are discarded and function symbols are demangled **once** and stored in simpler data structures. A symbol_table can be traversed using simple callbacks and method csdbg::symbol_table::foreach. The access to a symbol_table is not thread safe, the caller must implement thread synchronization.

Class csdbg::name_space

This class defines the way to group symbol tables of different objective code files (executables and DSO libraries), into a single object (the namespace) and perform **batch** symbol lookups on them. Inverse lookups are also supported (given a resolved symbol, find the **module** that defines it). A lookup cache is used internally to optimize symbol resolving. A `name_space` can be traversed (its symbol tables) using simple callbacks and method `csdbg::name_space::foreach`. The access to a `name_space` is not thread safe, the caller must implement thread synchronization.

1.6 6. Examples and tutorials

The examples come in a series of four programs of incremental complexity to cover as many of the features as possible. That's why the examples are treated as steps that the library user must follow, to understand the various tricks needed to correctly integrate `libcsdbg` and exploit it to the maximum. These programs will be dynamically linked with `libcsdbg.so` and with the example DSO `libcsdbg_test.so`, so their installation directories (**`$PREFIX/lib`** and **`$PREFIX/lib/modules/libcsdbg`**) must be in the `ld` path or in the **`$LD_LIBRARY_PATH`** shell variable. You may need to invoke the following line, before you run any of the examples:

```
export LD_LIBRARY_PATH=/usr/local/lib:/usr/local/lib/modules/libcsdbg
- or in generic -
export LD_LIBRARY_PATH=$PREFIX/lib:$PREFIX/lib/modules/libcsdbg
```

- **Example DSO** (`example/libcsdbg_test.cpp`) - This example is compiled into a **DSO** and linked with all of the example executables to demonstrate the flawless and easy integration of relocatable shared objects with `libcsdbg`, with either singlethreaded or multithreaded programs
- **First step** (`example/csdbg_step1.cpp`) - Demonstrates the way to integrate and use `libcsdbg` with a singlethreaded program, a DSO and a user defined exception type
- **Second step** (`example/csdbg_step2.cpp`) - This example shows the way `libcsdbg` works with multithreaded programs and a signal handler (for fatal signals) that generates process stack trace dumps
- **Third step** (`example/csdbg_step3.cpp`) - Demonstrates the use of multiple output interfaces to output traces to files and to sockets connected to LDP servers
- **Fourth step** (`example/csdbg_step4.cpp`) - This is the final all-inclusive example. It builds on all previous examples and demonstrates all `libcsdbg` tricks and features, from working with multithreaded programs and DSO, to doing output to files and LDP servers

The tutorial are the simplest possible programs, showing how to perform a simple single task, using one of the `libcsdbg` interfaces.

- **First tutorial** (`example/csdbg_tut1.cpp`) - Simple exception stack trace output to console
- **Second tutorial** (`example/csdbg_tut2.cpp`) - Simple thread stack trace output to console
- **Third tutorial** (`example/csdbg_tut3.cpp`) - Simple thread stack trace output to a file
- **Fourth tutorial** (`example/csdbg_tut4.cpp`) - Simple thread stack trace output to a client socket connected to an LDP server
- **Fifth tutorial** (`example/csdbg_tut5.cpp`) - This tutorial demonstrates the use of instrumentation plugins and plugin modules (DSO). The example plugin module (**`$PREFIX/lib/modules/libcsdbg/mod_null.so`**) must be visible from the dynamic linker, so its path must be declared in **`ld.so.conf`** or in the **`$LD_LIBRARY_PATH`** shell variable